BAB II
Tinjauan Pustaka

2.1 Literatur Review

Beberapa penelitian sebelumnya yang pernah membahas penelitian yang berkaitan yaitu penelitian yang dilakukan oleh Mohammad Alim Zulkifli (2018) yaitu melakukan analisis serangan DoS pada router menggunakan metode *Live* Forensic. Dalam penelitian yang dilakukannya, serangan DoS yang dianalisis adalah DNS Flooding yang dapat membuat jaringan router menjadi down disebabkan beban yang diterima tidak dapat ditampung. Hal tersebut dikarenakan serangan yang dilakukan memiliki karakteristik dapat melakukan Ping atau mengirimkan pesan tanpa henti. Dalam penelitian tersebut dilakukan monitoring menggunakan aplikasi Wireshark terkait adanya aktivitas yang tidak sesuai dengan proses komunikasi data pada protocol DNS dalam router pada rentan waktu tertentu. Proses akuisisi yang dilakukan melalui pendekatan metode Live Forensics disimpulkan bahwa adanya aktivitas tidak wajar dalam router yaitu pada proses komunikasi data.

Penelitian lain yang dilakukan oleh Mazdadi (2017) terkait analisis forensik pada RouterOS menggunakan metode Live Forensics yang mana dalam penelitian tersebut memanfaatkan media API *(Application Programming Interface) service* yang ada pada RouterOS untuk menggali informasi dari perangkat tersebut. API *(Application Programming Interface)* tersebut digunakan untuk membangun aplikasi yang bisa digunakan untuk berkomunikasi dengan router dengan memanfaatkan port 8726. Aplikasi tersebut akan digunakan dalam menjelaskan hasil identifikasi pada router terkait aktivitas yang terjadi pada router selama serangan berlangsung sebagai penerapan pendekatan metode Live Forensics. Adapun output yang dihasilkan dari penggunaan aplikasi tersebut berupa Log Activity, IP Address List, ARP, DHCP Leases, DNS Cache, dan Router Board Info yang kemudian dianalisis untuk mengungkapkan aktivitas illegal pada router.

Selain itu dalam penelitian yang dilakukan oleh Abdul Fadlil & Imam Riadi (2017) mengenai pengembangan system pengamanan jaringan computer berdasarkan analisis forensik jaringan maka dilakukan simulasi serangan menggunakan *software* LOIC untuk mengetahui kemampuan system pengaman jaringan computer yang dikembangkan. Selain itu, proses mendeteksi terjadinya serangan pada jaringan dilakukan dengan menggunakan aplikasi WinBox yang aplikasi tersebut dapat menunjukkan *resource*, IP Address penyerang, jumlah Paket Data serta waktu serangan terjadi.

Desti Mualfah & Imam Riadi (2017) melakukan penelitian di tahun yang sama yaitu tentang *Network Forensics for Detecting Flooding Attack on Web Server* menerangkan bahwa *web server* rentan terhadap ancaman serangan termasuk *Flooding Attack*. Dalam penelitian tersebut dilakukan scenario serangan menggunakan aplikasi LOIC serta aplikasi Snort sebagai aplikasi pendeteksi adanya serangan terhadap *log web server* serta menganalisis data log tersebut. Efek dari serangan tersebut menyebabkan hilangnya *bandwidth* dan kelebihan beban sehingga akses yang dilakukan oleh pengguna menjadi sulit. Dalam scenario serangan tersebut ditemukan 15 IP *address* yang melakukan tindakan illegal pada web server setelah dilakukan analisis. Dari penelitian tersebut berhasil mendeteksi adanya serangan pada *server web* dengan menggunakan pendekatan Metode *Live Forensics*.

Dalam penelitian yang dilakukan oleh Muhammad Sabri Ahmad, Imam Riadi, dan Yudi Prayudi (2017) terkait investigasi Live Forensics dari sisi pengguna untuk menganalisa serangan Man In The Middle Attack berbasis Evil Twin menjadi suatu ancaman bagi pengguna WiFi. Hal ini dikarenakan penyerangan tersebut memanfaatkan Access Point (AP) palsu dengan konfigurasi gateway yang berbeda dengan legitimate AP, sehingga menyebabkan jenis serangan ini sulit untuk dideteksi. Oleh karena itu, untuk mendeteksi aktivitas illegal yang terjadi dalam jaringan WiFi terkait kasus MITM Based Evil Twin Attack maka perlu dilakukan teknik forensik dengan menggunakan metode Live Forensics melalui pendekatan dari sisi user sehingga dapat membantu dalam menemukan informasi yang dapat menjadi petunjuk seperti IP Address, MAC Address pelaku serta temuan lainnya dengan melalui empat tahapan yaitu collection, examination, analysis dan reporting. Dari penelitian ini disimpulakan bahwa barang bukti digital dari serangan tersebut dapat diketahui dengan menganalisa atribut-atribut dari Access Point. Ada beberapa informasi yang dapat dijadikan perbandingan yaitu SSID, MAC Kode Vendor, kekuatan sinyal, Authentication, Frequency dan Channel. Penerapan metode Live Forensics dilakukan pada tahapan analisa dan pengumpulan barang bukti, hal ini dilakukan karena proses pengumpulan barang bukti dilakukan pada saat system sedang berjalan. Selain itu, pendekatan user-side cukup efektif dalam proses pengidentifikasian aktivitas serangan Evil Twin Based MITM.

Pada tahun yang sama penelitian yang dilakukan oleh Tayomi Dwi Larasati dan Bekti Cahyo Hidayanto (2017) melakukan penelitian terkait penerapan dan pengimplementasian teknik Live Forensics dalam mendapatkan bukti digital dan aktivitas penggunaan aplikasi Instant Messenger membutuhkan tools dan teknik yang berbeda untuk

mendapatkan analisa yang sesuai dengan yang diinginkan. Teknik dan tools untuk live forensics sendiri juga tidak dapat digunakan bersamaan, hal ini dikarenakan apabila RAM mati maka tidak dapat dilakukan dumping dan analisa barang bukti. Oleh sebab itu untuk pelaksanaan live forensics dibutuhkan metode baku agar dapat menjamin validitas dan integritas serta kelengkapan data yang dibutuhkan. Dari analisa ingin diketahui aplikasi yang mudah dan sulit untuk memperoleh data sebagai bukti digital. Dilakukan pengujian skenario dengan cara eksperimen berupa data percakapan biasa dan penghapusan pesan atau percakapan. Menggunakan tools Winhex dan Belkasoft Evidence Center digunakan untuk menganalisa data digital. Jenis data berupa data primer percakapan dan data media yang memiliki karakteristik unik sehingga data yang didapatkan juga berbeda bergantung struktur data yang disusun pada aplikasi. Berdasarkan analisa perbandingan data primer percakapan pada tools Winhex untuk 3 aplikasi tersebut sebesar 76%, 100%, dan 0% dan tools Belkasoft sebesar 10%, 20% dan 0%. Berdasarkan jumlah object yang dikirim dengan jumlah object yang terdeteksi pada tools Winhex sebesar 60,95%, 100%, dan 0%, untuk tools Belkasoft sebesar 6,67%, 33,33% dan 0%.

Penelitian yang dilakukan oleh Sony, Yudi Prayudi dan Bambang Sugiantoro (2017) mengenai teknik akuisisi virtualisasi server menggunakan metode live forensics menjelaskan bahwa virtualisasi server dapat mengundang celah kejahatan. Hal ini menjadi tantangan tersendiri dalam menemukan petunjuk dan bukti digital dalam mengungkapkan kasus kejahatan yang terjadi. Namun hal tersebut dapat menyulitkan penyidik untuk melakukan akuisisi terhadap salah satu system operasi yang ter-install di dalam server tanpa mengganggu ataupun mematikan computer mengingat pentingnya peran server tersebut. Dalam perkembangan saat ini dimana satu computer dapat memuat lebih dari satu system operasi sehingga diperlukan teknik akuisisi yang tepat dalam mengambil data yang diperlukan tanpa mengambil keseluruhan data dalam computer server tersebut. Mengingat prosese akuisisi yang akan dilakukan menggunakan metode live forensics sebab kondisi server fisik masih dalam keadaan berjalan. Dalam penelitian ini disimpulkan bahwa teknik akuisisi yang dilakukan untuk mengakuisisi salah satu virtual mesin yang terdapat pada server promox berhasil dilakukan karena salah satu partisi virtual mesin dalam server berhasil diakuisisi tanpa mengganggu system operasi lainnya. Adapun semua file yang ada dalam partisi tersebut dapat dibaca oleh software forensik dan beberapa file yang telah dihapus dapat ditemukan kembali.

Di tahun yang sama, Arif Wirawan Muhammad, Imam Riadi dan Sunardi (2017) melakukan penelitian terkait Deteksi Serangan DDoS menggunakan Neural Network

dengan fungsi Fixed Moving Average Window. Dalam penelitian ini dilakukan pengembangan sebuah pendekatan baru untuk mendeteksi serangan DDoS, berdasarkan pada karakteristik aktivitas jaringan menggunakan neural network dengan fungsi fixed moving average window (FMAW) sebagai metode deteksi. Data pelatihan dan pengujian diambil dari CAIDA DDoS Attack 2007 dan simulasi mandiri. Pengujian terhadap metode neural network dengan fungsi fixed moving average window (FMAW) menghasilkan presentase rata-rata pengenalan terhadap tiga kondisi jaringan (normal, slow DDoS dan DDoS) sebesar 90,52%. Untuk menghasilkan tingkat pengenalan yang lebih baik lagi, maka ada beberapa parameter yang dapat dioptimasi yaitu, memperbanyak jumlah data pelatihan, optimasi jumlah neuron dan hidden layer pada neural network, konfigurasi pelatihan neural network (momentum, learning rate, epoch, dan goal mean square error), penyesuaian fungsi pelatihan, dan fungsi aktivasi layer neural network. Adanya pendekatan baru dalam mendeteksi serangan DDoS, diharapkan bisa men jadi sebuah komplemen terhadap system IDS dalam meramalkan terjadinya serangan DDoS.

Penelitian lain terkait forensik jaringan dilakukan oleh Arif Roid Caesarano dan Imam Riadi (2018) melakukan penelitian forensik jaringan untuk mendeteksi serangan SQL Injection menggunakan metode NIST. Dalam penelitian tersebut penerapan system deteksi intrusion pada web server dapat digunakan untuk membantu mendeteksi serangan serta menghasilkan log terkait informasi penyerangan dan pemberitahuan serangan menggunakan tools Snort. Metode yang digunakan adalah NIST 800-30 dimana terdapat 9 tahapan penting dalam penilaian resiko. Dalam proses simulasi kasus yang dilakukan terdapat 5 tahapan yaitu pengujian kerentanan, scenario serangan, konfigurasi snort, pengumpulan data dan tahapan analisis. Hasil dari penelitian ini yaitu pengembangan system web server menggunakan Snort untuk system deteksi serangan SQL Injection dan notifikasi serangan real time menggunakan email.

Selain itu, Randi Rizal (2018) melakukan penelitian terkait forensik jaringan untuk mendeteksi serangan *Flooding* pada perangkat *Internet of Things* (IoT). Penelitian ini menggunakan model forensik jaringan untuk mendeteksi dan mengidentifikasi serangan. Dalam penelitian tersebut ditemukan bahwa ada 3 IP address yang melakukan tindakan illegal sehingga menyebabkan kelebihan pada lalu lintas data. Investigasi dilakukan pada file log dengan extensi p.cap yang didapatkan menggunakan aplikasi wireshark dan menemukan bahwa perangkat yang terinfeksi adalah perangkat IoT Bluetooth Arduino.

Paparan singkat terkait penelitian di atas, selengkapnya diuraikan dalam Tabel 2.1

Tabel 2.1 Literature Review

No	Nama	Judul	Metode Forensik	Tipe Serangan	Layer	Hasil
1.	Muhammad Alim Zulkifli, 2018	Live Forensics Method for Analysis Denial of Service (DoS) Attack on Routerboard	Live Forensics	DNS Flooding	Layer 7 (Application)	Serangan DoS yang dianalisis adalah DNS Flooding yang dapat membuat jaringan router menjadi down disebabkan beban yang diterima tidak dapat ditampung. Hal tersebut dikarenakan serangan yang dilakukan memiliki karakteristik dapat melakukan Ping atau mengirimkan pesan tanpa henti. Dalam penelitian tersebut dilakukan monitoring menggunakan aplikasi Wireshark terkait adanya aktivitas yang tidak sesuai dengan proses komunikasi data pada protocol DNS dalam router pada rentan waktu tertentu.
2.	Muhammad Itqan Mazdadi, 2017	Live Forensics on RouterOS using API Services to Invetigate Network Attack	Live Forensics	Brute Force	Layer 4 (Transport)	API *(Application Programming Interface)* digunakan untuk membangun aplikasi yang bisa digunakan untuk berkomunikasi dengan router dengan memanfaatkan port 8726. Aplikasi tersebut akan digunakan dalam menjelaskan hasil identifikasi pada router terkait aktivitas yang terjadi pada router selama serangan berlangsung sebagai penerapan pendekatan metode Live Forensics. Adapun output yang dihasilkan dari penggunaan aplikasi tersebut berupa Log Activity, IP Address List, ARP, DHCP Leases, DNS Cache, dan Router Board Info yang kemudian dianalisis untuk mengungkapkan aktivitas illegal pada router.

3.	Abdul Fadlil & Imam Riadi, 2017	Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan	Live Forensics	HTTP Flooding	Layer 7 (Application)	Proses mendeteksi terjadinya serangan pada jaringan dilakukan dengan menggunakan aplikasi WinBox yang aplikasi tersebut dapat menunjukkan *resource*, IP Address penyerang, jumlah Paket Data serta waktu serangan terjadi.
4.	Desti Mualfah & Imam Riadi, 2017	Network Forensics For Detecting Flooding Attack On Web Server	Live Forensics	UDP Flooding	Layer 4 (Transport)	Dalam penelitian tersebut dilakukan scenario serangan menggunakan aplikasi LOIC serta aplikasi Snort sebagai aplikasi pendeteksi adanya serangan terhadap *log web server* serta menganalisis data log tersebut. Efek dari serangan tersebut menyebabkan hilangnya *bandwidth* dan kelebihan beban sehingga akses yang dilakukan oleh pengguna menjadi sulit. Dalam scenario serangan tersebut ditemukan 15 IP *address* yang melakukan tindakan illegal pada web server setelah dilakukan analisis. Dari penelitian tersebut berhasil mendeteksi adanya serangan pada *server web* dengan menggunakan pendekatan Metode *Live Forensics*.
5.	Muhammad Sabri Ahmad, Imam Riadi, dan Yudi Prayudi, 2017	Investigasi Live Forensics dari sisi pengguna untuk menganalisa serangan *Man In The Middle Attack* berbasis *Evil Twin*	Live Forensics	MITM Attack	Layer 1 (Physical), Layer 2 (Data Link)	Barang bukti digital dari serangan tersebut dapat diketahui dengan menganalisa atribut-atribut dari *Access Point*. Ada beberapa informasi yang dapat dijadikan perbandingan yaitu *SSID, MAC Kode Vendor,* kekuatan sinyal, *Authentication*, *Frequency* dan *Channel.* Penerapan metode Live Forensics dilakukan pada tahapan analisa dan pengumpulan barang bukti, hal ini dilakukan karena proses pengumpulan barang bukti

						dilakukan pada saat system sedang berjalan. Selain itu, pendekatan *user-side* cukup efektif dalam proses pengidentifikasian aktivitas serangan *Evil Twin Based MITM.*
6.	Tayomi Dwi Larasati dan Bekti Cahyo Hidayanto, 2017	Analisis *Live Forensics* untuk Perbandingan Aplikasi *Instant Messenger* pada System Operasi Windows 10	Live Forensics	-	-	Dari analisa ingin diketahui aplikasi yang mudah dan sulit untuk memperoleh data sebagai bukti digital. Dilakukan pengujian skenario dengan cara eksperimen berupa data percakapan biasa dan penghapusan pesan atau percakapan. Menggunakan tools Winhex dan Belkasoft Evidence Center digunakan untuk menganalisa data digital. Jenis data berupa data primer percakapan dan data media yang memiliki karakteristik unik sehingga data yang didapatkan juga berbeda bergantung struktur data yang disusun pada aplikasi. Berdasarkan analisa perbandingan data primer percakapan pada tools Winhex untuk 3 aplikasi tersebut sebesar 76%, 100%, dan 0% dan tools Belkasoft sebesar 10%, 20% dan 0%. Berdasarkan jumlah object yang dikirim dengan jumlah object yang terdeteksi pada tools Winhex sebesar 60,95%, 100%, dan 0%, untuk tools Belkasoft sebesar 6,67%, 33,33% dan 0%.
7.	Sony, Yudi Prayudi dan Bambang Sugiantoro, 2017	Teknik Akuisisi Virtualisasi Server Menggunakan Metode Live Forensics	Live Forensics	-	-	Dalam penelitian ini disimpulkan bahwa teknik akuisisi yang dilakukan untuk mengakuisisi salah satu virtual mesin yang terdapat pada server promox berhasil dilakukan karena salah

						satu partisi virtual mesin dalam server berhasil diakuisisi tanpa mengganggu system operasi lainnya. Adapun semua file yang ada dalam partisi tersebut dapat dibaca oleh software forensik dan beberapa file yang telah dihapus dapat ditemukan kembali.
8.	Arif Wirawan Muhammad, Imam Riadi dan Sunardi, 2017	Deteksi Serangan DDoS menggunakan Neural Network dengan fungsi Fixed Moving Average Window.	Live Forensics	-	-	Pengujian terhadap metode neural network dengan fungsi fixed moving average window (FMAW) menghasilkan presentase rata-rata pengenalan terhadap tiga kondisi jaringan (normal, slow DDoS dan DDoS) sebesar 90,52%. Untuk menghasilkan tingkat pengenalan yang lebih baik lagi, maka ada beberapa parameter yang dapat dioptimasi yaitu, memperbanyak jumlah data pelatihan, optimasi jumlah neuron dan hidden layer pada neural network, konfigurasi pelatihan neural network (momentum, learning rate, epoch, dan goal mean square error), penyesuaian fungsi pelatihan, dan fungsi aktivasi layer neural network. Adanya pendekatan baru dalam mendeteksi serangan DDoS, diharapkan bisa men jadi sebuah komplemen terhadap system IDS dalam meramalkan terjadinya serangan DDoS.
9.	Arif Roid Caesarano dan Imam Riadi, 2018	Forensik jaringan untuk mendeteksi serangan SQL Injection menggunakan metode NIST	Live Forensics	SQL Injection	Layer 7 (Application)	Dalam proses simulasi kasus yang dilakukan terdapat 5 tahapan yaitu pengujian kerentanan, scenario serangan, konfigurasi snort, pengumpulan data dan tahapan analisis. Hasil dari penelitian ini yaitu pengembangan system web

						server menggunakan Snort untuk system deteksi serangan SQL Injection dan notifikasi serangan real time menggunakan email.
10.	Randi Rizal, 2018	Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device	Live Forensics	TCP Flooding	Layer 4 (Transport)	Dalam penelitian tersebut ditemukan bahwa ada 3 IP address yang melakukan tindakan illegal sehingga menyebabkan kelebihan pada lalu lintas data. Investigasi dilakukan pada file log dengan extensi p.cap yang didapatkan menggunakan aplikasi wireshark dan menemukan bahwa perangkat yang terinfeksi adalah perangkat IoT Bluetooth Arduino.

Berbeda dengan penelitian sebelumnya, dalam penelitian ini Network Forensics dengan menggunakan metode Live Forensics dimana objek yang diteliti adalah Router Mikrotik. Paparan singkat mengenai penelitian ini seperti tertulis pada Tabel 2.2

Tabel 2.2 Penelitian Yang Diusulkan

Judul	**Uraian Singkat Masalah Penelitian**	**Solusi**	**Hasil yang Diharapkan**
Forensik Router untuk Mendeteksi Flooding Attack Menggunakan Metode Live Forensic	Melakukan explorasi terhadap Router Mikrotik untuk menemukan bukti digital yang dapat menjadi informasi dalam proses investigasi forensik jaringan, serta bagaimana proses pendeteksian terkait serangan pada router dan menentukan karakteristik serangan berdasarkan temuan dalam proses investigasi	Memanfaatkan aplikasi Wireshark dan Winbox sebagai media dalam mendeteksi serangan Flooding secara Live Forensics dan memanfaatkan Tools Metasploit sebagai media untuk melakukan simulasi serangan Flooding pada Router	1. Dapat mengetahui informasi yang ditemukan pada router sebagai bukti digital. 2. Memudahkan dalam mendeteksi serangan Flooding menggunakan aplikasi Wireshark 3. Melakukan akuisisi data menggunakan metode Live Forensics untuk mendapatkan informasi yang digunakan sebagai bukti digital Forensics dan juga karakteristik dari serangan pada router.

2.2 Tinjauan Pustaka

2.2.1 Network Forensic

Network forensic merupakan salah satu cabang ilmu yang mempelajari keamanan jaringan termasuk menyelidiki serangan yang terjadi pada sebuah jaringan berdasarkan bukti digital yang ditemukan di lokasi kejadian. Bukti digital yang ditemukan kemudian akan diidentifikasi untuk mengetahui serangan yang dilakukan oleh penyerang. Serangan tersebut antara lain Probing, DDoS, User to Root (U2R) dan Remote to Local.

Network Forensic atau yang disebut forensic jaringan merupakan proses menangkap, mencatat dan menganalisa aktivitas pada suatu jaringan guna menemukan jejak digital atau bukti digital dari suatu serangan atau kejahatan yang dilakukan menggunakan jaringan computer sehingga pelaku penyerangan atau kejahatan dapat dituntut sesuai hokum yang berlaku, (Mukkamala, et al, 2003). Bukti digital dapat ditemukan dengan mengidentifikasi pola serangan, penyimpangan dari perilaku normal jaringan ataupun penyimpangan dari kebijakan yang telah diterapkan pada suatu jaringan. Dalam forensic jaringan terdapat berbagai aktivitas dan teknik analisis. Beberapa contoh diantaranya analisis dari proses pada *Network Intrusion Detection System* (NIDS), analisis pada lalu lintas jaringan hingga analisis pada piranti jaringan juga termasuk dalam bagian dari forensic jaringan.

2.2.2 Live Forensic

Live Forensics merupakan keadaan atau proses analisis forensic yang dilakukan disaat system yang dianalisis sementara dalam keadaan sedang berjalan atau beroperasi, (Artformatics, 2013). Metode yang dilakukan dan filosofi pendekatannya adalah sama dengan proses Forensik tradisional, namun ketika system mati proses, terhenti dan dilanjutkan dengan menggunakan proses forensik tradisional/biasa, (Casey, 2010).

Live forensic dilakukan untuk mencari informasi dan barang bukti dalam sebuah jaringan local, artinya kita menghadapi suatu keadaan dimana computer atau alat bukti yang ditemui di tempat kejadian perkara terhubung pada sebuah jaringan computer dan dalam keadaan *Power* On, (Casey, 2010). Metode ini dilakukan karena informasi yang dapat menjadi sebuah bukti digital memiliki kemungkinan dapat hilang apabila system yang di analisis berada dalam keadaan mati. Selain itu, hal ini memberikan keuntungan dari kekurangan proses forensik tradisional yang tidak dapat menganalisa sebuah jaringan computer untuk mencari barang bukti serta informasi didalamnya, (Dimaio, 2001).

Menurut (Dimaio, 2001) setiap metode maupun cara yang dilakukan pasti ada kekurangan dan kelebihannya masing-masing, tidak terkecuali pada metode *Live Forensics*, kelemahan pada *Live Forensics*, meliputi:

a. Berbedanya instalasi setiap Komputer, keterbatasan pengetahuan ataupun keahlian yang dimiliki oleh seorang analisis Forensik akan menjadi sebuah hambatan karena *Environment* setiap komputer berbeda sistem operasinya dan perangkat *Hardwarenya*.
b. Kemungkinan data termodifikasi dan mempengaruhi akuisisi data untuk disajikan pada saat persidangan kasus penyerangan jaringan.
c. Berkaitan dengan File gambar yang akan mengalami kompresi ketika akan diambil atau dipindahkan mempengaruhi kualitas dari gambar tersebut dan akan menjadi sulit untuk diidentifikasi pada saat melakukan analisa ataupun ketika dihadirkan pada saat persidangan.
d. Bukti yang diambil dari jaringan menjadi barang bukti yang tidak terpercaya karena kemungkinan hadirnya teknik Anti Forensik yang dapat mengelabui seorang investigator.
e. Data yang diambil dalam sebuah jaringan menjadi sebuah data yang Korup, sehingga mengurangi akuisisi barang bukti.

Pengaruh positif yang dimiliki *Live Forensics* yaitu ketika teknik Forensik tradisional tidak mampu mengambil data atau informasi dalam suatu jaringan.

2.2.3 Router

Router merupakan perangkat utama yang bertujuan untuk mengatur lalu lintas jaringan dari satu system ke system lainnya. Router memanfaatkan alamat IP untuk memindahkan data. Perangkat ini bekerja pada lapisan tiga dari OSI Layer. Dalam konteks level jaringan, kita dapat berhadapan dengan topologi logis jaringan dimana kita memperoleh alamat IP (Kurniawan, 2012).

Router merupakan sebuah system operasi berbasis linux yang difungsikan sebagai network Router. System ini didesain untuk memberikan kemudahan bagi penggunanya. Proses administrasinya bisa dilakukan melalui aplikasi lain seperti WinBox. Router memiliki kemampuan melewatkan paket IP Address dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya. Router yang saling terhubung dalam jaringan internet turut serta dalam sebuah algoritma routing terdistribusi untuk menentukan jalur terbaik yang dilalui paket IP Address dari system ke system lain, (Zulkifli, 2018).

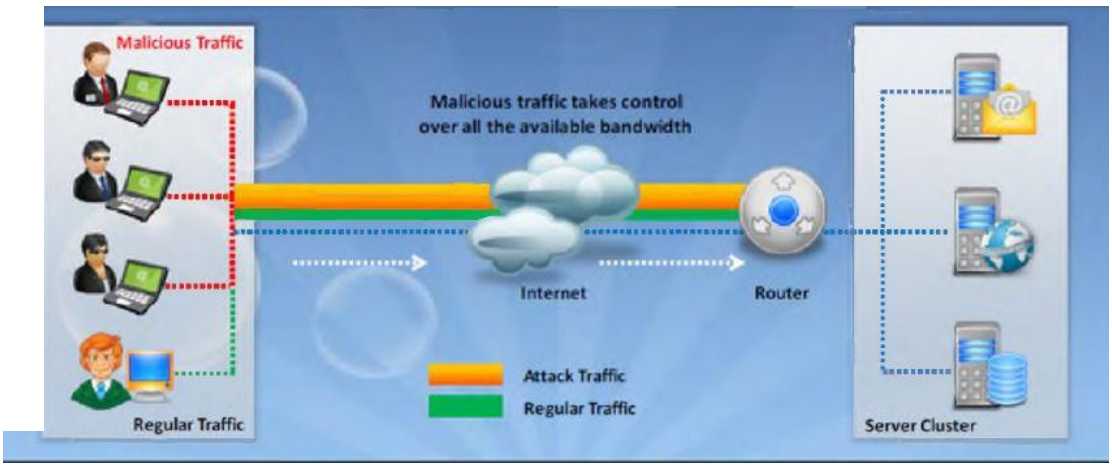
Router memiliki berbagai fungsi, beberapa fungsi tersebut diantaranya :

a. Membaca alamat logika IP Address *source* dan *destination* untuk menentukan routing dari suatu LAN ke LAN lainnya.
b. Menyimpan routing *table* untuk menentukan *rute* terbaik antara LAN ke WAN.
c. Perangkat di layer 3 OSI Layer. d. Bisa berupa box atau sebuah OS yang menjalankan sebuah *deamon* routing.
d. Interfaces Ethernet, Serial, ISDN BRI.

2.2.4 Flooding Attack

Flooding Attack atau Serangan Flooding terdiri dari DoS *(Denial of Service)* dan DDoS *(Distributed Denial of Service)*. DoS merupakan jenis serangan di dalam sebuah jaringan dimana target dalam serangan tersebut adalah sebuah computer atau server dengan tujuan mematikan layanan computer atau server tersebut. Sedangkan DDoS merupakan salah satu jenis serangan DoS yang menggunakan banyak computer untuk menyerang sebuah server dalam suatu jaringan secara bersama.

Pada dasarnya serangan DoS *(Denial of Service)* bersifat “satu lawan satu”, sehingga dibutuhkan sebuah *host* yang kuat demi membanjiri lalu lintas host target sehingga mencegah klien yang valid untuk mengakses layanan jaringan pada server yang dijadikan target serangan. Serangan DDoS ini menggunakan teknik yang lebih canggih dibandingkan dengan serangan *Denial of Service* yang klasik, yakni dengan meningkatkan serangan beberapa kali dengan menggunakan beberapa buah komputer sekaligus, sehingga dapat mengakibatkan server atau keseluruhan segmen jaringan dapat menjadi "*tidak berguna sama sekali*" bagi klien.



Gambar 2.1 Serangan DoS.

Serangan Flooding akan mencoba untuk mencegah akses pengguna terhadap system atau jaringan dengan menggunakan beberapa cara diantaranya sebagai berikut :

1. Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut sebagai *traffic flooding*.
2. Membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disedakan oleh sebuah host sehingga request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini disebut sebagai *request flooding*.
3. Mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan server.

Tipe serangan DoS *(Denial of Service)* dalam bentuk awal adalah serangan *Syn Flooding Attack*, yang pertama kali muncul pada tahun 1996 dan mengeksploitasi terhadap kelemahan yang terdapat di dalam protocol *Transmission Control Protocol* (TCP). Serangan-serangan lainnya akhirnya dikembangkan untuk mengeksploitasi kelemahan yang terdapat di dalam system operasi, layanan jaringan atau aplikasi untuk menjadikan sistem, layanan jaringan, atau aplikasi tersebut tidak dapat melayani pengguna, atau bahkan mengalami *crash*. Beberapa tool yang digunakan untuk melakukan serangan DoS pun banyak dikembangkan setelah itu (bahkan beberapa tool dapat diperoleh secara bebas), termasuk di antaranya Bonk, LAND, Smurf, Snork, WinNuke, dan Teardrop.

Meskipun demikian, serangan terhadap TCP merupakan serangan DoS yang sering dilakukan. Hal ini disebabkan karena jenis serangan lainnya (seperti halnya memenuhi ruangan hard disk dalam sistem, mengunci salah seorang akun pengguna yang valid, atau memodifikasi tabel routing dalam sebuah router) membutuhkan penetrasi jaringan terlebih dahulu, yang kemungkinan penetrasinya kecil, apalagi jika sistem jaringan tersebut telah diperkuat.

2.2.5 Metasploit

Metasploit saat ini adalah tool pengujian penetrasi terkemuka di dunia, dan salah satu proyek open-source terbesar dalam keamanan informasi dan pengujian penetrasi. Tool ini merevolusi cara kita untuk melakukan tes keamanan pada sistem kita. Alasan Metasploit begitu populer adalah berbagai tugas yang dilakukannya dapat memudahkan pekerjaan dalam melakukan pengujian penetrasi untuk membuat sistem lebih aman. Metasploit tersedia untuk semua sistem operasi. Proses kerjanya untuk semua system operasi hampir sama. Berikut ini pengenalan singkat terkait framework dan terminology yang terkait dengan metasploit antara lain :

a. Metasploit Framework merupakan framework pengujian penetrasi open-source gratis yang dilakukan pertama kali oleh H. D. Moore pada tahun 2003, yang kemudian diakuisisi oleh Rapid7. Versi stabil dari kerangka ini ditulis menggunakan bahasa Ruby. Ini memiliki basis data teruji yang terbesar di dunia dan menerima lebih dari satu juta unduhan setiap tahun. Selain itu merupakan salah satu proyek paling kompleks yang dibangun di Ruby hingga saat ini.
b. Vulnerability adalah kelemahan yang memungkinkan penyerang / pentester untuk membobol atau membahayakan keamanan sistem. Kelemahan ini ada di sistem operasi, perangkat lunak aplikasi, atau bahkan dalam protokol jaringan.
c. Exploit adalah bagian dari kode yang memungkinkan penyerang / penguji untuk mengambil keuntungan dari sistem yang rentan dan membahayakan keamanannya. Setiap kerentanan memiliki eksploitas yang sesuai. Metasploit memiliki lebih dari 1.700 eksploitasi.
d. Payload adalah kode aktual yang melakukan pekerjaan. Payload berjalan pada sistem setelah eksploitasi. Sebagian besar digunakan untuk mengatur koneksi antara mesin penyerang dan korban. Metasploit memiliki lebih dari 500 payload.
e. Module adalah blok bangunan kecil dari sebuah sistem yang lengkap. Setiap modul melakukan tugas tertentu dan sistem yang lengkap dibangun dengan menggabungkan beberapa modul yang berfungsi sebagai satu kesatuan. Keuntungan terbesar dari arsitektur semacam itu adalah memudahkan bagi pengembang untuk mengintegrasikan kode dan alat eksploitasi baru ke dalam kerangka kerja.

Metasploit menggunakan library yang berbeda dan sebagai pemegang kunci untuk berfungsinya framework. Library ini adalah kumpulan tugas, operasi, dan fungsi yang telah ditetapkan dan dapat digunakan oleh berbagai modul framework. Bagian paling mendasar dari framework ini adalah library dengan ekstensi Ruby (Rex). Beberapa komponen yang disediakan oleh Rex termasuk implementasi klien protokol dan server, subsistem logging, utilitas eksploitasi classes, dan lainnya. Rex sendiri dirancang untuk tidak memiliki ketergantungan, selain dari apa yang ada pada instalasi Ruby default.

2.2.6 Wireshark

Wireshark adalah sebuah aplikasi analisis paket jaringan. Aplikasi ini akan mencoba untuk menangkap paket jaringan dan mencoba menampilkan dalam bentuk data sedetail mungkin. *Wireshark* merupakan salah satu dari sekian banyak *tools network analyzer* yang banyak digunakan oleh network administrator untuk menganalisa kinerja jaringannya termasuk

protokol didalamnya. *Wireshark* banyak disukai karena interface-nya yang menggunakan *Graphical User Interface* (GUI) atau tampilan grafis. *Wireshark* mampu menangkap paket-paket data atau informasi yang melewati jaringan.semua jenis paket informasi dalam berbagai format protocol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang *tools* ini juga dapat dipakai untuk *sniffing* (memperoleh informasi penting seperti *password* email atau *account* lain) dengan menangkap paketpaket yang melewati jaringan dan menganalisanya, (Sarsono, 2012).